TELKOMNIKA, Vol.16, No.2, April 2018, pp. 811~826
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v16i2.8507

Research on 4-dimensional Systems without Equilibria with Application

Ruibin Hao*[1], Lequan Min[2], Hongyan Zang[3]
Schools of Mathematics and Physics, University of Science and Technology Beijing, Beijing China, 100083
*Corresponding author, e-mail: haoruibin0001@163.com, minlequan@sina.com, zhylixiang@126.com

Abstract

Recently chaos-based encryption has been obtained more and more attention. Chaotic systems without equilibria may be suitable to be used to design pseudorandom number generators (PRNGs) because there does not exist corresponding chaos criterion theorem on such systems. This paper proposes two propositions on 4-dimensional systems without equilibria. Using one of the propositions introduces a chaotic system without equilibria. Using this system and the generalized chaos synchronization (GCS) theorem constructs an 8-dimensional discrete generalized chaos synchronization (8DBDGCS) system. Using the 8DBDGCS system designs a 216-word chaotic PRNG. Simulation results show that there are no significant correlations between the key stream and the perturbed key streams generated via the 216-word chaotic PRNG. The key space of the chaotic PRNG is larger than 21275. As an application, the chaotic PRNG is used with an avalanche-encryption scheme to encrypt an RGB image. The results demonstrate that the chaotic PRNG is able to generate the avalanche effects which are similar to those generated via ideal chaotic PRNGs.

Keywords: *chaotic map, pseudorandom number generator, randomness test, avalanche encryption scheme*

1. Introduction

Chaos is a kind of complex dynamic behaviors generated from determined nonlinear systems. Chaotic behaviors are extremely sensitive to initial conditions, difficult to predict in a long-term [1-3]. Chaos synchronization (CS) is of essential importance for many physical, biological and engineering systems. Pecora and Carroll's poineer work on GS communication [4] has made the research on GS to developed rapidly [5-11]. The apparant random behaviors of chaotic systems makes them to provide new tools for cryptography and other fields [12-25].

In cryptographic terms, the strict key avalanche criterion means that when any bit of the key change, each binary bit of the ciphertext should have a change with the probability of one half [26,27]. In 2013, a d-bit segment stream encryption scheme with avalanche effect (SESAE) has been presented [28]. The feature of the SESAE is to make each bit of the decrypted plaintext changed to 1 with probability of $(2^d-1)/2^d$ if using an ideal d-bit PRNG [28]. Following [28], some 2^{16}-word PRNGs have been designed [19,29,30], which provide a new tool in cryptography.

Dynamic chaotic systems without equilibria have generally complex dynamic behaviors [31], and more suitable to design PRNGs because there are corresponding chaos criterion theorems on them. In a recent paper [19], we have firstly intorduded a kind of disrete chaotic system without equilibria (DCSE), used a DCSE to design a PRNG applying to SESAE.

Conseqently, studing new theorems on DCSE, PRNGs and their applications to SESAE is important both for theoretical researchs and pactical applications. This paper firstly set up two new propositions for determining 4-dimensional DCSE. Our propositions extend the results obtained in [19]. And then introduces such a DCSE. Thirdly construct an DCSE-based generalized CS (GCS) system, and simulate the complex dynamics of the system. Fourthly designs a DCSE-GCS-based PRNG. and uses the NIST FIPS 140-2 test suite [32] to test the randomness of the GCS PRNG, the RC4 algorithm and the ZUC algorithm [33]. Finally, using the GCS PRNG and the SESAE [28] encrypts an RGB image with numerical analysis.

Received January 4, 2018; Revised January 21, 2018; Accepted February 16, 2018

2. Definition and the GCS Theorem

Definition 1: (Similar to [34,35]).*Consider two systems,*

$$\mathbf{X}(k+1) = F(\mathbf{X}(k)) \tag{1}$$

$$\mathbf{Y}(k+1) = G(\mathbf{Y}(k), \mathbf{X}(k)) \tag{2}$$

where

$$\mathbf{X}(k) = (x_1(k), \mathrm{L}\ , x_n(k))^{\mathrm{T}} \tag{3}$$

$$\mathbf{Y}(k) = (y_1(k), \mathrm{L}\ , y_m(k))^{\mathrm{T}}, m \le n \tag{4}$$

$$F(\mathbf{X}(k)) = (f_1(\mathbf{X}(k)), \mathrm{L}\ , f_n(\mathbf{X}(k)))^{\mathrm{T}} \tag{5}$$

$$G(\mathbf{Y}(k), \mathbf{X}(k)) = (g_1(\mathbf{Y}(k), \mathbf{X}(k)), \mathrm{L}\ , g_m(\mathbf{Y}(k), \mathbf{X}(k)))^{\mathrm{T}}. \tag{6}$$

If there exists a transformation

$$H : ¡^{n} \to ¡^{m} \tag{7}$$

$$H(\mathbf{X}(k)) = (h_1(\mathbf{X}(k)), \mathrm{L}\ , h_m(\mathbf{X}(k)))^{\mathrm{T}} \tag{8}$$

and a subset $B = B_X \times B_Y \subset ¡^{n} \times ¡^{m}$ such that all trajectories of (1) and (2) with initial conditions in B satisfy $\lim_{k \to +\infty} \| H(\mathbf{X}(k)) - \mathbf{Y}(k) \| = 0$, then the two systems (1) and(2) are said to be in GS with respect to the transformation $H(\mathbf{X}(k))$. System (1) is called the driving system, while system (2) is the driven system. In particular, if the two systems are chaotic, then the GS is called a generalized chaos synchronization (GCS).

In order to construct a new discrete chaotic system with the GCS property, the following theorem is needed.

Theorem 1: [11] *Let* $\mathbf{X}, \mathbf{Y}, \mathbf{X}_m, F(\mathbf{X})$ *and* $G(\mathbf{Y}, \mathbf{X})$ *be defined by (3)-(6), and* $\mathbf{X}_m = (x_1(k), \mathrm{L}\ , x_m(k))^{\mathrm{T}}$

Suppose that

$$H(\mathbf{X}_m) = (y_1, y_2, \mathrm{L}\ , y_m)^{\mathrm{T}} \tag{9}$$

is an invertible transformation. If the two systems (1) and (2) are in GCS via the transformation $\mathbf{Y} = H(\mathbf{X}_m)$, then the function $G(\mathbf{Y}, \mathbf{X})$ given in (2) will have the following form:

$$G(\mathbf{Y}, \mathbf{X}) = H(F_m(\mathbf{X})) - q(\mathbf{X}_m, \mathbf{Y}) \tag{10}$$

Where

$$F_m(\mathbf{X}) = (f_1(\mathbf{X}), f_2(\mathbf{X}), \mathrm{L}\ , f_m(\mathbf{X}))^{\mathrm{T}}$$

and the function

$$q(\mathbf{X}_m, \mathbf{Y}) = (q_1(\mathbf{X}_m, \mathbf{Y}), q_2(\mathbf{X}_m, \mathbf{Y}), \mathrm{L}\ , q_m(\mathbf{X}_m, \mathbf{Y}))^{\mathrm{T}}$$

guarantees that the zero solution of the following error equation is asymptotically stable:

$$\mathbf{e}(k+1) = H(\mathbf{X}_m(k+1)) - \mathbf{Y}(k+1) = q(\mathbf{X}_m, \mathbf{Y}) \tag{11}$$

3. Two Propositions on Chaotic System Without Equilibria

Consider a general parametric form of four-dimensional discrete system:
Form A:

$$\begin{cases} x_1(k+1) = x_1(k) + f_1(x_1(k), x_2(k), \alpha_1) \\ x_2(k+1) = f_2(x_1(k), x_2(k), x_3(k), x_4(k), \alpha_2, \alpha_3, \alpha_4) \\ x_3(k+1) = x_3(k) + f_3(x_1(k), x_2(k), \alpha_5, \alpha_6) \\ x_4(k+1) = x_4(k) + f_4(x_1(k), x_2(k)) \end{cases} \tag{12}$$

Where $a_i \in ¡^{n}, i = 1,2,\mathrm{L}\ ,6.$ Now we give the following
Proposition 1: If the following conditions hold, then system (12) has no equilibrium.

i $f_1(x_1, x_2, a_1) = 0$ if and only if $x_1 = x_2$

ii $f_3(x_1(k), x_2(k), a_5, a_6) = 0$ if and only if $x_1 x_2 = a_6^2$

iii $f_4(a_6, a_6) \neq 0$

Proof. Firstly, solve for the equilibrium of the first equation of system (12). Condition (i) gives

$$\begin{aligned} x_1(k) &= x_1(k) + f_1(x_1(k), x_2(k), a_1) \\ x_1(k) &= x_2(k) \end{aligned} \tag{13}$$

Substituting (13) into the third equation of system (12) and letting $x_3(k+1) = x_3(k)$ gives

$$0 = f_3(x_1(k), x_2(k), a_5, a_6) \tag{14}$$

and

$$x_1(k) = x_2(k) = a_6 \tag{15}$$

Then substituting (15) into the fourth equation of system(12) and letting $x_4(k+1) = x_4(k)$ gives

$$0 = f(a_6, a_6) \neq 0 \tag{16}$$

This contradiction shows that system (12) has no equilibria. This completes the proof.
Form B:

$$\begin{cases} x_1(k+1) = \dfrac{g(x_1(k), x_2(k), x_3(k), x_4(k)) + e(x_1(k), x_2(k), x_3(k), x_4(k))}{f_1(x_1(k), x_2(k), x_3(k), x_4(k))} \\ x_2(k+1) = \dfrac{g(x_1(k), x_2(k), x_3(k), x_4(k))}{f_2(x_1(k), x_2(k), x_3(k), x_4(k)} \\ x_3(k+1) = x_3(k) + \dfrac{\sin(\beta_1 x_1(k))}{f_3(x_1(k), x_2(k), x_3(k), x_4(k))} \\ x_4(k+1) = x_4(k) + \dfrac{\sin(\beta_2 x_2(k))}{f_3(x_1(k), x_2(k), x_3(k), x_4(k))} \end{cases} \tag{17}$$

where $\beta_1, \beta_2 \neq 0$. Now we give the following
Proposition 2: If the following conditions hold, then system (17) has no equilibrium.

i $|g(x_1(k),x_2(k),x_3(k),x_4(k))|<M$

ii $0<|e(x_1(k),x_2(k),x_3(k),x_4(k))|<N$

iii $f_i(x_1(k),x_2(k),x_3(k),x_4(k))\geq\alpha_i>0, i=1,2,3,4.$

iv $|\frac{\pi}{\beta_1}|>\frac{M+N}{\alpha_1}$, $|\frac{\pi}{\beta_2}|>\frac{M}{\alpha_2}$

Proof. Solving the equilibrium point is to solve the following Equations:

$$\begin{cases} x_1(k)=\dfrac{g(x_1(k),x_2(k),x_3(k),x_4(k))+e(x_1(k),x_2(k),x_3(k),x_4(k))}{f_1(x_1(k),x_2(k),x_3(k),x_4(k))} & (18-1)\\ x_2(k)=\dfrac{g(x_1(k),x_2(k),x_3(k),x_4(k))}{f_2(x_1(k),x_2(k),x_3(k),x_4(k))} & (18-2)\\ 0=\dfrac{\sin(\beta_1 x_1(k))}{f_3(x_1(k),x_2(k),x_3(k),x_4(k))} & (18-3)\\ 0=\dfrac{\sin(\beta_2 x_2(k))}{f_4(x_1(k),x_2(k),x_3(k),x_4(k))} & (18-4) \end{cases} \quad (18)$$

Then $sin(\beta_1 x_1(k))=0$, because of (18-3) and conditions (iii). Those imply

$$\beta_1 x_1(k)=m\pi, m=0,\pm1,\pm2\mathrm{L}$$

then

$$x_1(k)=\frac{m\pi}{\beta_1}, m=0,\pm1,\pm2\mathrm{L}$$

And we can know $|x_1(k)|<\frac{M+N}{\alpha_1}$ form the proposition 2

that is

$$|\frac{m\pi}{\beta_1}|<\frac{M+N}{\alpha_1}, m=0,\pm1,\pm2,\mathrm{L} \quad (19)$$

then $m=0$ because of (19) and condition (iv), so $x_1(k)=0$ and similarly $x_2(k)=0$.
then

$$\begin{cases} g(0,0,x_3(k),x_4(k))+e(0,0,x_3(k),x_4(k))=0\\ g(0,0,x_3(k),x_4(k))=0 \end{cases}$$

then

$$0=e(0,0,x_3(k),x_4(k))>0$$

This contradiction shows that system (17) has no equilibria. This completes the proof.

Table 1 shows fourteen systems which satisfy propositions 1 and 2, respectively. The corresponding Lyapunov exponents and initial conditions are listed in the table. The largest Lyapunov exponents of all systems are positive. Therefore they are chaotic systems. The chaotic orbits of the state variables $x_1(k)$, $x_2(k)$, $x_3(k)$ and $x_4(k)$ of the systems are shown in Figure 1 and Figure 2. It can be observed that, although the same initial conditions are used, the chaotic systems have different dynamical characteristics.

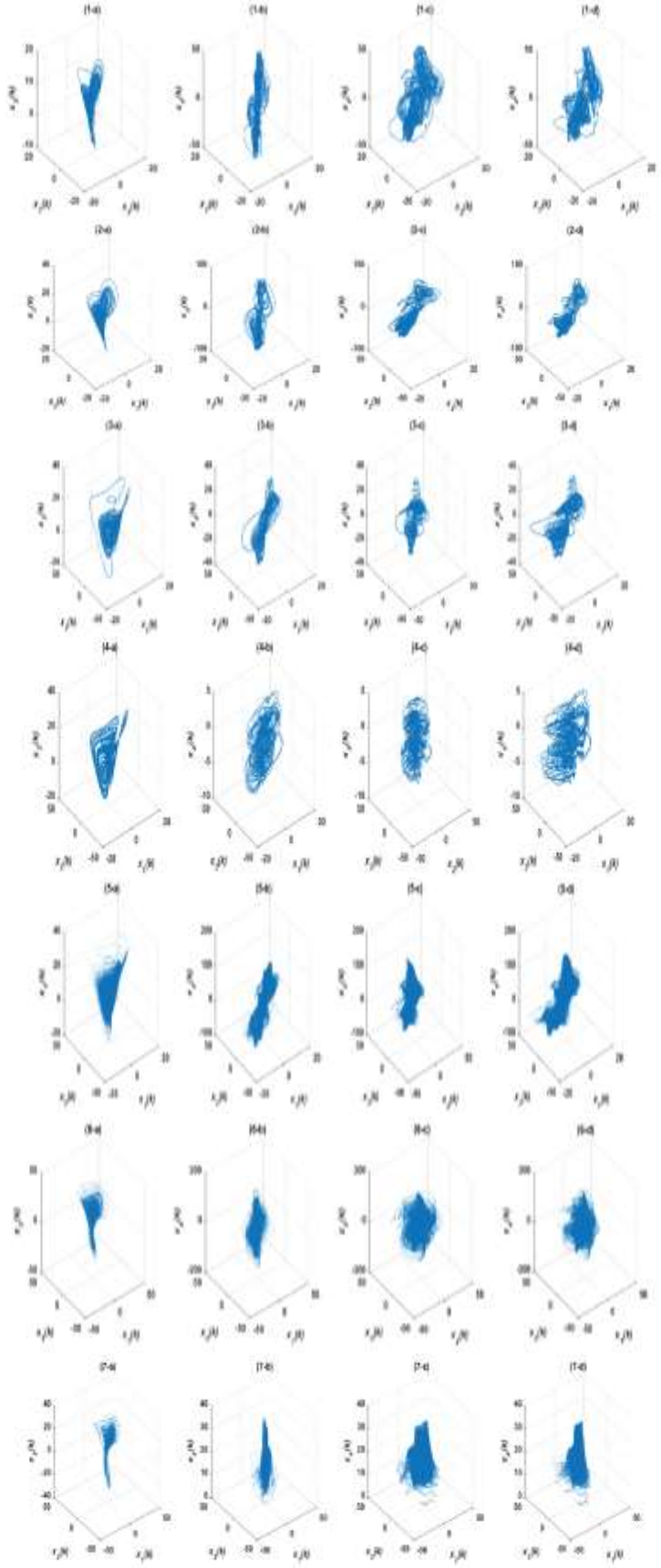

Figure 1. Chaotic orbits of the variables of the form a listed in Table 1

Table 1. 4-dimensional Discrete Chaotic Systems without Equilibrium

Number	Form A	LEs	Form B	LEs	X(0)
1	$x_1(k+1)=x_1(k)+0.01(x_2(k)-x_1(k))$	0.00065	$x_1(k+1)=\frac{\sin(6x_3(k))+e^{-0.6x_1(k)^2}}{x_4(k)^2+2}$	0.1964	0.5
	$x_2(k+1)=1.0025x_2(k)-0.0012x_1(k)x_3(k)+0.001x_4(k)$	0	$x_2(k+1)=\frac{\sin(6x_3(k))}{x_1(k)^2+1}$	0.0127	0.4
	$x_3(k+1)=x_3(k)+0.001(x_1(k)x_2(k)-20)$	0.00065	$x_3(k+1)=x_3(k)+\frac{\sin(2x_1(k))}{\sin(x_2(k))^2+1}$	0.0405	0.3
	$x_4(k+1)=x_4(k)+0.1\sin(x_2(k))$	0.00746	$x_4(k+1)=x_4(k)+\frac{\sin(3x_2(k))}{x_3(k)^2+1}$	2.2677	0.2
2	$x_1(k+1)=x_1(k)+0.01(x_2(k)-x_1(k))$	0.00097	$x_1(k+1)=\frac{\cos(6x_3(k))+e^{-0.6x_1(k)^2}}{\sin(x_4(k))^2+2}$	0.1189	0.5
	$x_2(k+1)=1.0035x_2(k)-0.001x_1(k)x_3(k)+0.001x_4(k)$	0	$x_2(k+1)=\frac{\cos(6x_3(k))}{0.5\sin(x_1(k))^2+1}$	0.0213	0.4
	$x_3(k+1)=x_3(k)+0.001(x_1(k)x_2(k)-25)$	0.00174	$x_3(k+1)=x_3(k)+\frac{\sin(2x_1(k))}{\sin(x_2(k))^2+1.5}$	0.3766	0.3
	$x_4(k+1)=x_4(k)+0.1\sin(x_1(k))$	0.00566	$x_4(k+1)=x_4(k)+\frac{\sin(3x_2(k))}{0.5x_3(k)^2+0.5}$	2.3302	0.2
3	$x_1(k+1)=x_1(k)+0.01(x_2(k)-x_1(k))$	0.00055	$x_1(k+1)=\frac{\sin(6x_3(k))+0.01e^{-0.6\sin(x_4(k))^2}}{x_4(k)^2+2}$	0.1495	0.5
	$x_2(k+1)=1.0025x_2(k)-0.001x_1(k)x_3(k)+0.001x_4(k)$	0	$x_2(k+1)=\frac{\sin(6x_3(k))}{x_1(k)^2+1}$	0.0196	0.4
	$x_3(k+1)=x_3(k)+0.001(x_1(k)x_2(k)-25)$	0.00041	$x_3(k+1)=x_3(k)+\frac{\sin(2x_1(k))}{x_2(k)^2+1.5}$	0.2296	0.3
	$x_4(k+1)=x_4(k)+0.01\sin(x_1(k))+0.01\sin(x_2(k))$	0.00759	$x_4(k+1)=x_4(k)+\frac{\sin(3x_2(k))}{x_3(k)^2+1}$	1.3294	0.2
4	$x_1(k+1)=x_1(k)+0.01(x_2(k)-x_1(k))$	0.00101	$x_1(k+1)=\frac{\sin(7x_3(k))+0.01e^{-5\sin(x_4(k)x_2(k))^2}}{x_4(k)^2+2}$	0.1554	0.5
	$x_2(k+1)=1.0035x_2(k)-0.001x_1(k)x_3(k)+0.0005x_4(k)$	0	$x_2(k+1)=\frac{\sin(7x_3(k))}{x_1(k)^2+1.5}$	0.0750	0.4
	$x_3(k+1)=x_3(k)+0.001(x_1(k)x_2(k)-25)$	0.00011	$x_3(k+1)=x_3(k)+\frac{\sin(2x_1(k))}{x_2(k)^2+2}$	0.2807	0.3
	$x_4(k+1)=x_4(k)+0.01\sin(x_1(k))\cos(x_2(k))$	0.00746	$x_4(k+1)=x_4(k)+\frac{\sin(3x_2(k))}{x_3(k)^2+1}$	2.1360	0.2
5	$x_1(k+1)=x_1(k)+0.1(x_2(k)-x_1(k))$	0.01409	$x_1(k+1)=\frac{\sin(7x_3(k))+0.1e^{-5\sin(x_2(k)x_4(k))^2}}{x_4(k)^2+2}$	0.1204	0.5
	$x_2(k+1)=1.025x_2(k)-0.01x_1(k)x_3(k)+0.01x_4(k)$	0	$x_2(k+1)=\frac{\sin(7x_3(k))}{x_1(k)^2+1}$	0.0182	0.4
	$x_3(k+1)=x_3(k)+0.01(x_1(k)x_2(k)-25)$	0.09350	$x_3(k+1)=x_3(k)+\frac{\sin(2x_1(k))}{x_2(k)^2+2}$	0.2617	0.3
	$x_4(k+1)=x_4(k)+0.1\sin(x_1(k))^2+2\sin(x_1(k))$	0.07182	$x_4(k+1)=x_4(k)+\frac{\sin(3x_2(k))}{x_3(k)^2+1}$	1.4264	0.2
6	$x_1(k+1)=x_1(k)+0.1(x_2(k)-x_1(k))$	0.01220	$x_1(k+1)=\frac{0.9\sin(9x_3(k))+e^{-0.6x_1(k)^2}}{x_4(k)^2+2}$	0.2201	0.5
	$x_2(k+1)=1.005x_2(k)-0.01x_1(k)x_3(k)+0.005x_4(k)$	0.00015	$x_2(k+1)=\frac{0.9\sin(9x_3(k))}{x_1(k)^2+1}$	0.0077	0.4
	$x_3(k+1)=x_3(k)+0.01(x_1(k)x_2(k)-25)$	0.00954	$x_3(k+1)=x_3(k)+\frac{\sin(2x_1(k))}{\sin(x_2(k))^2+1.5}$	0.2811	0.3
	$x_4(k+1)=x_4(k)+0.01e^{\sin(x_2(k))}+1.5\sin(x_1(k))$	0.09662	$x_4(k+1)=x_4(k)+\frac{\sin(3x_2(k))}{0.5x_3(k)^2+2.5}$	2.5885	0.2
7	$x_1(k+1)=x_1(k)+0.1(x_2(k)-x_1(k))$	0.00387	$x_1(k+1)=\frac{\sin(7x_3(k))+0.1e^{-4\sin(x_4(k))^2}}{x_4(k)^2+2}$	0.3657	0.5
	$x_2(k+1)=1.005x_2(k)-0.01x_1(k)x_3(k)+0.005x_4(k)$	0	$x_2(k+1)=\frac{\sin(7x_3(k))}{x_1(k)^2+1}$	0.0597	0.4
	$x_3(k+1)=x_3(k)+0.01(x_1(k)x_2(k)-30)$	0.00155	$x_3(k+1)=x_3(k)+\frac{\sin(3x_1(k))}{2\sin(x_2(k))^2+2}$	0.6234	0.3
	$x_4(k+1)=x_4(k)+0.05\sin(x_1(k))x_2(k)$	0.09704	$x_4(k+1)=x_4(k)+\frac{\sin(2x_2(k))}{\sin(x_3(k))^2+1.5}$	-1.655	0.2

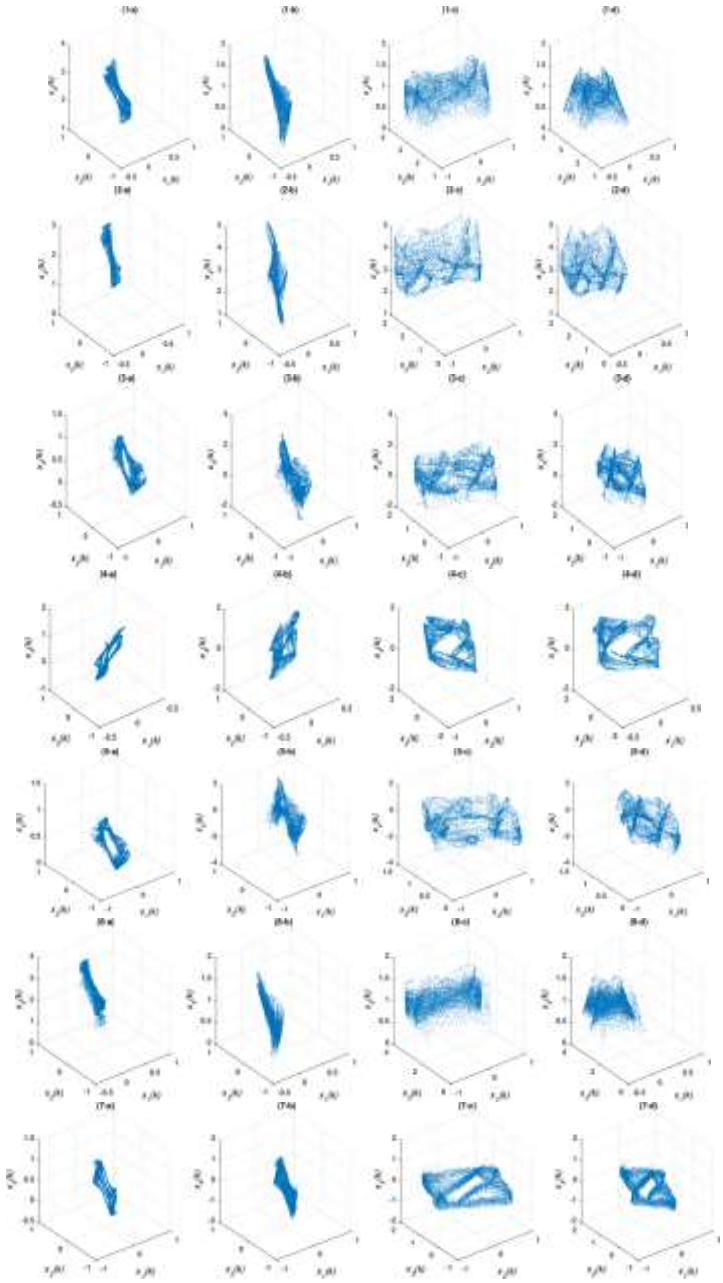

Figure 2. Chaotic orbits of the variables of the form b listed in Table 1

4. A chaotic System-Based GCS Theorem

Firstly, we construct a 4-dimensional polynomial system

$$\mathbf{X}=\begin{cases} x_1(k+1)= & x_1(k)+0.01(x_2(k)-x_1(k)) \\ x_2(k+1)= & 1.0025x_2(k)-0.001x_1(k)x_3(k)+0.001x_4(k) \\ x_3(k+1)= & x_3(k)+0.001(x_1(k)x_2(k)-25) \\ x_4(k+1)= & x_4(k)+0.1\sin(x_2(k)). \end{cases} \tag{20}$$

From Proposition 1, system (20) has no equilibria. Calculated Lyapunov exponents of this system are $\{0.00104,\ 0,-0.00089,\ -0.00761\}$. Therefore, it is chaotic. System (20) is used as the driving system of our GCS system.

Second construct an invertible matrix:

$$A = \begin{pmatrix} 4 & 2 & 8 & 7 \\ 5 & 8 & 3 & 1 \\ 7 & 0 & 2 & 3 \\ 4 & 3 & 1 & 7 \end{pmatrix} \tag{21}$$

with the transformation $H : ¡^4 \to ¡^4$ defined as follows:

$$H(\mathbf{X}) = A\mathbf{X} \ @(h_1(\mathbf{X}), h_2(\mathbf{X}), h_3(\mathbf{X}), h_4(\mathbf{X})) \tag{22}$$

Let

$$q(\mathbf{X}, \mathbf{Y}) = \frac{1}{8}(\mathbf{AX} - \mathbf{Y}) \tag{23}$$

where $q(\mathbf{X}, \mathbf{Y})$ is used to ensure the error Equation (11) be asymptotically stable.
Using Theorem 1, we can select a driven system as following form:

$$\mathbf{Y}(k+1) = \begin{pmatrix} y_1(k+1) \\ y_2(k+1) \\ y_3(k+1) \\ y_4(k+1) \end{pmatrix} = \mathbf{A}[F(\mathbf{X}(k))] - q(\mathbf{X}(k), \mathbf{Y}(k)). \tag{24}$$

Therefore system (20) and (24) are in GCS with respect to transformation (22). Now choose (25) and (26) as initial conditions:

$$\mathbf{X}(0) = (0.2, 0.1, 0.75, -2)^{\mathrm{T}} \tag{25}$$

$$\mathbf{Y}(0) = \mathbf{AX}(0) \tag{26}$$

The numerical simulated chaotic orbits of state variables x_1, x_2, x_3, x_4 and y_1, y_2, y_3, y_4 for the first 50000 iterations are shown in Figure 3 and Figure 4, respectively. The evolution of state variables: $k - x_1(k)$, $k - x_2(k)$, $k - x_3(k)$, $k - x_4(k)$ and $k - y_1(k)$, $k - y_2(k)$, $k - y_3(k)$, $k - y_4(k)$ are shown in Figure 5 and Figure 6. It can be observed that the dynamic behaviors of the chaotic system demonstrate chaotic attractor. Moreover, as the theory predicts, with respect to transformation $H = A\mathbf{X}(k)$ and $\mathbf{Y}(k)$ are showed in generalized synchronization in Figure 7.

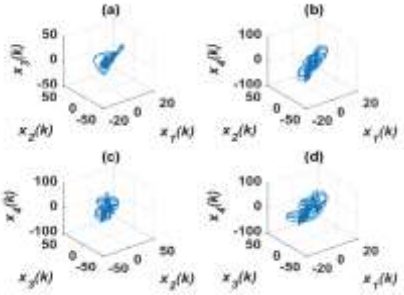

Figure 3. Chaotic trajectories of variables: (a) $x_1(k)-x_2(k)-x_3(k)$,(b) $x_1(k)-x_2(k)-x_4(k)$ (c) $x_1(k)-x_3(k)-x_4(k)$,(d) $x_2(k)-x_3(k)-x_4(k)$

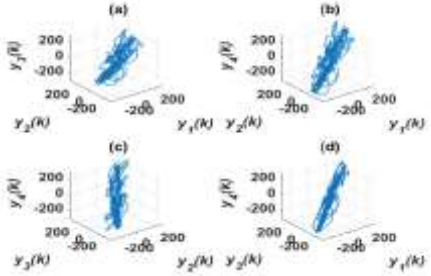

Figure 4. Chaotic trajectories of variables: (a) $y_1(k)-y_2(k)-y_3(k)$,(b) $y_1(k)-y_2(k)-y_4(k)$ (c) $y_1(k)-y_3(k)-y_4(k)$,(d) $y_2(k)-y_3(k)-y_4(k)$

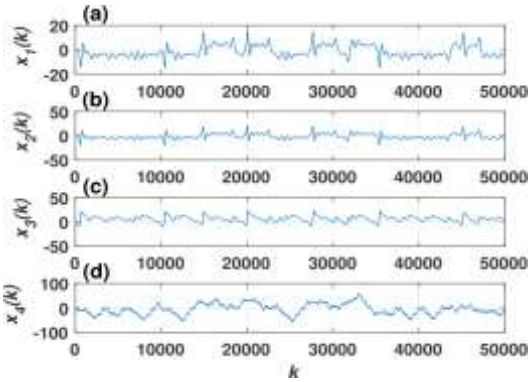

Figure 5. The evolution of state variables: (a) $k-x_1(k)$ (b) $k-x_2(k)$ (c) $k-x_3(k)$ (d) $k-x_4(k)$

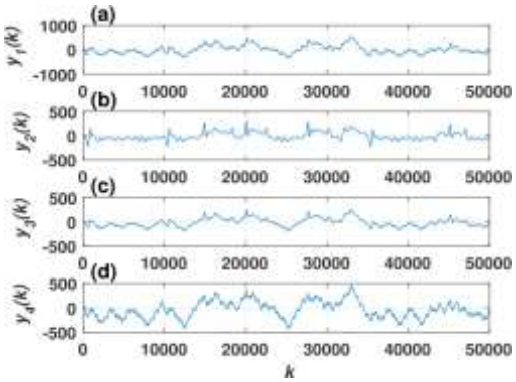

Figure 6. The evolution of state variables: (a) $k-y_1(k)$ (b) $k-y_2(k)$ (c) $k-y_3(k)$ (d) $k-y_4(k)$

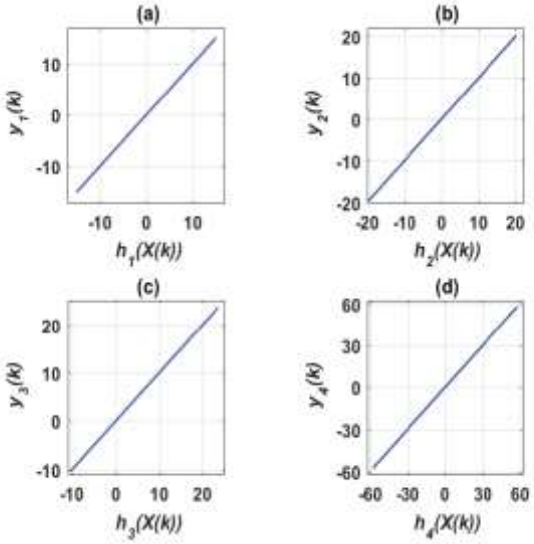

Figure 7. The state vectors and are in generalized synchronization with respect to the: (a), (b), (c), (d)

5. Chaotic Pseudorandom Number Generator and Pseudorandomness tests

5.1. Pseudorandom Number Generator

Denote

$$\begin{cases} \mathbf{X}_i = \{x_i(k) \mid i = 1,2,3,4\}, \\ \mathbf{Y}_i = \{y_i(k) \mid i = 1,2,3,4\} \end{cases} \tag{27}$$

where $x_{i'}s$, $y_{i'}s$ are defined by system (20) and (24).

Now introduce a transformation $T_1 : ¡ \to \{0,1,\mathrm{L}\ , 2^{16}-1\}$, which transforms the chaotic streams of systems(27) into key streams. Let $L = 10^{15}$, $S = X_3 + Y_1$ .Then, the chaotic PRNG T_1 is defined by

$$T_1(\mathbf{S}) = \mathrm{mod}(\mathrm{round}((L(\mathbf{S} - \min(\mathbf{S})) / (\max(\mathbf{S}) - \min(\mathbf{S}))), 2^{16}) \tag{28}$$

The seeds of the chaotic PRNG are the initial conditions of the GCS system, which can be chosen via random number generator. Therefore, the output key streams of the chaotic PRNG can be obtained via the transformation (28) on the chaotic streams of the GCS systems (20) and (24).

5.2. Pseudorandomness Test

The FIPS 140-2 test consists of four sub-tests: Monobit Test, Poker Test, Runs Test and Long Runs Test. Each test needs a single stream of 20,000 one and zero bits from the keystream generator. Any failure in the first three tests means that the corresponding quantity of the sequences falls out the required intervals listed in the second column of Table 2. The Long Runs test is passed if there are no runs of length 26 or more.

Two previous papers [36,37] have pointed out that the required intervals of Monobit test and Porker test correspond significant $\alpha = 10^{-4}$ for the normal cumulative distribution and the χ^2 distribution, respectively; however the required intervals of the Runs tests correspond approximately the significant $\alpha = 1.6 \times 10^{-7}$ for the normal cumulative distribution. If one selects the significant $\alpha = 10^{-4}$ of all tests, the corresponding accepted intervals are those as ones listed in the third column of Table 2 [36-37]. Then, we denote the accepted intervals by G FIPS 140-2 test criterion.

Table 2. The Required Intervals of FIPS 140-2 Monobit Test, Porker Tests, Runs Test. Here, MT, PT, and LT Represent the Monobit Test, the Porker Test and the Long Runs Test, k Represents the Length of the Run of a Tested Sequence. χ^2 DT Represents χ^2 Distribution

Test Item	FIPS 140-2 required intervals	$\alpha = 10^{-4}$ Accepted Intervals	Golomb's Postulates
MT	9,725~10,275	9,725_10,275	10000
PT	2.16~46.17	2.16_46.17	χ^2 DT
LT	< 26	< 26	----
k	Run Test	Run Test	Run Test
1	2,315~2,685	2,362~2,638	2,500
2	1,114~1,386	1,153~1,347	1,250
3	527~723	556~694	625
4	240~384	264~361	313
5	103~209	122~191	156
6+	103~209	122~191	156

According to Golomb's three postulates on the randomness, the ideal pseudorandom sequences should satisfy [38], the ideal values of the first three tests should be listed in the fourth column of Table 2. Finally, FIPS 140-2 test suite is used to test the randomness performance. One needs to change the keystreams with values $\{0,1,\mathrm{L}\ , 2^{16}-1\}$ to binary keystreams via the following transformation:

$$T: \{0,1,\mathrm{L}\ ,2^{16}-1\} \to \{0,1\}$$

which is defined by

$$T = T_{22} \circ T_{21} \tag{29}$$

$$\mathbf{y} \in \{0,1,\mathrm{L}\ ,2^{16}-1\}^{N}$$

$$T_{21}(\mathbf{y}) = dec2bin(\mathbf{y})$$

Let $\mathbf{z} = dec2bin(\mathbf{Y})$. Then

$$T_{22}(\mathbf{z}) = \mathbf{z}(:)$$

where $dec2bin$ and $\mathbf{z}(:)$ are both Matlab commands.

The FIPS 140-2 test is used to check 1,000 keystreams randomly generated, respectively by the chaotic PRNG with perturbed randomly initial conditions (25) and (26) and the matrix (21) in the range $|\dot{o}| \in [10^{-16},1]$. All sequences pass the FIPS 140-2 test and 16 sequences fail to pass the G FIPS 140-2 test. The test results are listed in the third column of Table 3, which the results are described by mean values ± standard deviation (Mean ± SD).

Table 3. The Confident Intervals of FIPS 140-2 Tested Values of 1,000 key Streams Generated by the CHAOTIC PRNG, the RC4 and ZUC PRNG. Here, SD Represents the Standard Deviation

Test item	bits	PRNG Mean ± SD	RC4 Mean ± SD	ZUC Mean ± SD
MT	0	9999.0 ± 69.813	9999.7 ± 70.092	9998.4 ± 71.843
	1	10000.9 ± 69.813	10000 ± 70.092	1002 ± 71.843
PT	-	15.175 ± 5.568	14.87 ± 5.433	15.043 ± 5.549
LT	0	13.577 ± 1.841	13.6 ± 1.8214	13.605 ± 1.841
	1	13.642 ± 1.930	13.604 ± 1.884	13.595 ± 1.931
1	0	2500.3 ± 45.770	2500.9 ± 45.568	2501.9 ± 45.735
	1	2498.7 ± 46.972	2501.4 ± 46.398	2502.7 ± 45.121
2	0	1249.4 ± 31.030	1250.5 ± 31.372	1252.1 ± 32.606
	1	1250.9 ± 31.613	1249 ± 31.048	1249.5 ± 32.221
3	0	624.42 ± 23.051	624.95 ± 22.964	624.09 ± 22.648
	1	625.58 ± 22.912	625.65 ± 22.93	624.64 ± 23.455
4	0	312.75 ± 16.662	311.71 ± 16.548	312.56 ± 16.748
	1	313.73 ± 16.245	312.17 ± 16.822	312.72 ± 16.506
5	0	156.36 ± 11.758	156.41 ± 12.069	155.65 ± 12.097
	1	155.99 ± 12.096	156.6 ± 11.958	156.66 ± 12.369
6+	0	156.13 ± 11.811	156.15 ± 11.792	155.75 ± 11.719
	1	156.53 ± 11.551	155.79 ± 11.979	155.82 ± 11.497

The Rivest Cipher 4 (RC4) has been widely used in popular protocols such as Secure Sockets since it's designed in 1987. The RC4 algorithm as PRNG can be designed via the Matlab commands which is shown in Figure 8.

Figure 8. The Matlab commands of RC4 algorithm to design PRNG

Here, “randint(1, 2^L, [0 2^L-1])” generates a vector of uniformly distributed random integers $\{0,1,\mathrm{L}\ ,2^L-1\}$ of dimension 2^L; “mod” means modulus after division; “zeros(1, N)” is a zero raw vector of dimension N. Consequently, the RC4 algorithm based L-bit segment PRNG is designed. Next, using FIPS 140-2 test to test the 1,000 keystreams randomly generated by RC4 PRNG. Results show that 1 and 12 sequences fail to pass the FIPS 140-2 test and G FIPS 140-2 test, respectively. The statistic test results are listed in the forth column of Table 3.

Furthermore, ZUC is a stream cipher that forms the heart of the third generation partnership project (3GPP) confidentiality algorithm 128-EEA3 and the 3GPP integrity algorithm 128-EIA3. Then, using FIPS 140-2 test to test the 1,000 keystreams randomly generated by the ZUC algorithm [33]. It demonstrates that all of the sequences pass the FIPS 140-2 test, and 21 sequences fail to pass the G FIPS 140-2 test. The test results are listed in the fifth column of Table 3. Finally, compare all test results shown in Table 3. It can be observed, the statistical properties of the pseudorandomness of the sequences generated via the three PRNGs don't have significant differences.

5.3. Key Space

The key parameters set of the proposed CHAOTIC PRNG includes the initial condition $\mathbf{X}(0)$, $\mathbf{Y}(0)$ and the matrix $A=(\alpha_{i,j})$. It can be proved that if the perturbation matrix $\Delta=(\delta_{i,j})$ satisfies $|\delta_{i,j}|<1.0035$, the matrix $A+\Delta$ is still invertible. Therefore the chaotic PRNG have 4+4+16 key
parameters denoted by

$$\mathbf{K}_s=\{k_1,k_2,\mathrm{L}\ ,k_{24}\} \tag{30}$$

The perturbed keys have the forms

$$\mathbf{K}_s(\Delta)=\mathbf{K}_s+[\delta_1,\delta_2,\mathrm{L}\ ,\delta_{24}] \tag{31}$$

The Matlab platform uses double precision decimal computations. That means each computed decimal number has 16 bits' accuracy. Therefore, one can select $10^{-16}\le|\delta_i|\le 1, i=1,\mathrm{L}\ ,24,$ that is, $\delta_i=0.a_1a_2\mathrm{L}\ a_{16}$, where $a_i\in[0,1,\mathrm{L}\ ,9]$. Therefore, the 24 keys have a key space which is larger than $10^{24\times16}>2^{1275}$. Now, compare the difference between the key stream S with 20000 codes length generated by the key set (30) with the key streams S_p generated by the perturbed key set (31), respectively.

The comparison results are shown in the third column of Table 4, where SV denotes the statistic values, DC denotes the different codes, and CC denotes the correlation coefficients. Observe that the average percent of different codes is 50.0136%, which is very closed to the ideal value 50%. And the average of the correlation coefficients is 0.00583440, also very closed to the ideal value of 0.

Table 4. The Statistic Data Describes the Percentages of the Codes of the Key Stream Variations between s and s_p as well as s and s_m

Item	SV	S_p	S_m
DC	Min	48.5900%	48.7299%
	Mean	50.0136%	49.9855%
	Max	51.1000%	51.0700%
CC	Min	00000871	0.00001005
	Mean	0.00583440	0.00554509
	Max	0.02823380	0.02533419

Next, compare the same key stream S with the 1000 streams S_m generated by the Matlab function randi([0 1], 1, 20000). The comparison results are shown in the fourth column of Table 4. Observe that the average percentage of different codes is 49.9855% and the average of the correlation coefficients is 0.00554509. The results suggest that the key stream S has no significant correlations with the perturbed key streams S_p and the streams S_m. In summary, the effective key space of the CHAOTIC PRNG is 10^{24x16} (larger than 2^{1275}), which is larger than the key space 10^{24x15} obtained in [19].

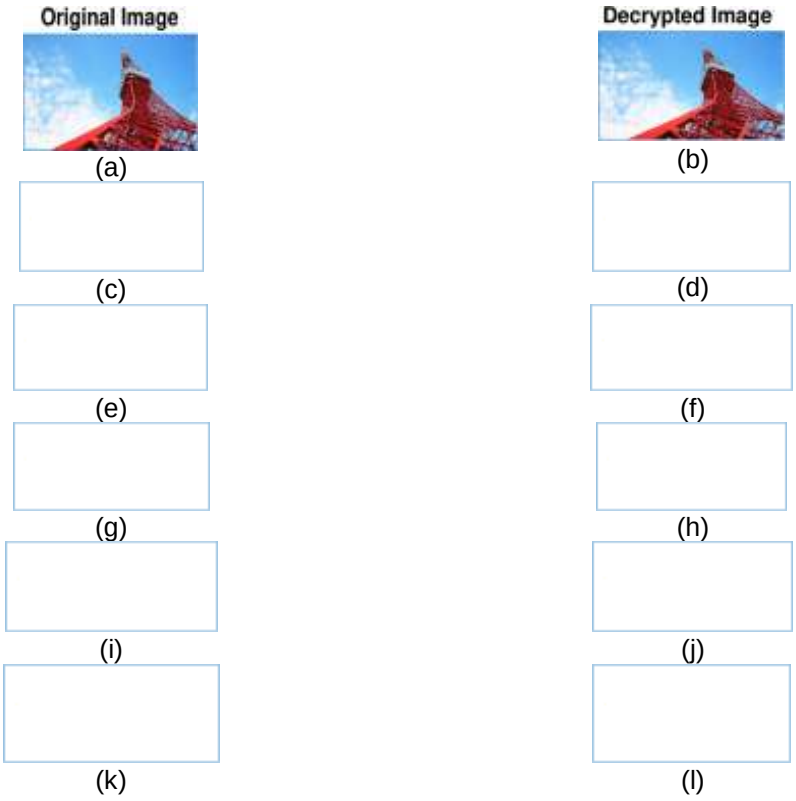

Figure 9 (a) Original Image (b) Decrypted Image via the key Streams P .Ten Decrypted Images via Key Streams Generated with Slighted Perturbed Initial Conditions and the Matrix within the Range $[10^{-15},10^{-10}]$: (c) $I_{1,1}$ (d) $I_{3,1}$ (e) $I_{4,1}$ (f) $I_{4,2}$,(g) $I_{5,1}$,(h) $I_{23,1}$ (i) $I_{23,2}$ (j) $I_{24,1}$,(k) $I_{24,2}$ and (l) $I_{25,1}$

6. Simulations on SESAE

Consider the avalanche effect of the CHAOTIC PRNG, which is used to encrypt an RGB image "tower" with 250×140 pixels. The simulation is implemented via the Matlab R2016a platform. The SESAE experiments on CHAOTIC PRNG are described as follows: Prosedures (1)-(4) are the same as those given in [19]. The receiver randomly disturbs the initial conditions

(25) and (26), and also the matrix (21), for 1000 times in the range $|\delta| \in [10^{-15}, 10^{-10}]$, then obtain disturbed key streams:

$$P_i, i = 1, 2, \text{L}\ , 1000. \tag{32}$$

The receiver uses $P_i = \{p_1, p_2, \text{L}\ , p_N\}$ to decrypt the ciphertext and obtains a decrypted plaintext:

$$\overline{M_i} = E^{-1}(C, P_i), i = 1, 2, \text{L}\ , 1000. \tag{33}$$

After changing $\bar{M}_i's$ to RGB images, one can find that all images become almost pure white-colored ones. There are $840000\{0,1\}$ codes in each decrypted image. Among the decrypted images,the minimum of $0's$ is 2 and the maximum of $0's$ is 24.

Denote $I_{i,j}$ the j th image that has i zero codes. The first five images with minimum zero codes and the last five images with maximum zero codes are shown in Figure 9(c)-(l). Therefore, the percentages of the numbers of "1" codes in the 1000 decrypted images are within the range $[0.999970, 0.999998]$, which are near to the ideal value $(2^{16} - 1)/2^{16} = 0.999985$, and are similar to those given in [19].

Table 5 lists some statistical data of the norms between the original key stream S_0 and the key stream $S_{i,j}$ used in the above ten decrypted images, respectively. The results suggest that there are no significant correlations between the norms and the corresponding decrypted image, and similar to those obtained in [19].

Table 5. Differences between the Original Keystream S_0 and the keysteams $S_{j,i}$, Measured by Norm $\| S_0 - S_{j,i} \|$

$\| S_0 - S_{j,i} \| \times 10^{-10}$					
	$S_{1,1}$	$S_{3,1}$	$S_{4,1}$	$S_{4,2}$	$S_{5,1}$
S_0	3.151	2.836	3.138	2.344	2.723
	$S_{23,1}$	$S_{23,2}$	$S_{24,1}$	$S_{24,2}$	$S_{25,1}$
S_0	3.092	2.828	2.847	2.950	2.817

Remark: To resist attacks, one may consider implementing an "one-time-pad" scheme into CHAOTIC PRNG: Let $\mathbf{X}$ be a set in the seed space (initial conditions) of the CHAOTIC PRNG, and assume that Alice and Bob share a one-to-one map $f: \mathbf{X} \to \mathbf{X}$. Before each communication, Alice randomly selects an element $x \in \mathbf{X}$ and sends it to Bob. Then, they both use $f(x)$ as the seed for one-time encryption.

In summary, the simulation shows that using the CHAOTIC PRNG and SESAE to encrypt RGB images is able to generate encrypted images with significant avalanche effects.

7. Concluding Remarks

The main results of this paper are summarized as follows:

a. This paper proposes two propositions on 4-dimensional discrete systems without equilibra, which extend the results obtained by [19].
b. A 4-dimensional discrete chaotic system is proposed. Using the system and the GS theorem designs an 8-dimensional GCS system.
c. Using the 8-dimensional GCS system constructs a chaotic PRNG. The key space of our PRNG is $10^{24 \times 16}$ (larger than 2^{1275}) is larger than the key space $10^{24 \times 15}$ obtained in [19] and the key space 2^{128} obtained by the ZUC algorithm.

d. Using the FIPS 140-2 test critrions tests the keystreams generated via the CHAOTIC PRNG, the RC4 algorithm and the ZUC algorithm. The results show that the randomness of the sequences generated via the chaotic PRNG and others are similar.
e. Numerical simulations show that the CHAOTIC PRNG is able to generate significant avalanche effects, and the percentages of the "1" code in the decrypted texts for different keystreams are larger than 0.999970, which is very closed to the idea value of $(2^{16}-1)/2^{16}=0.999985$ and similar to those given in [19]. Therefore, it verifies the proposed chaotic PRNG is a qualified candidate for SESAE.

In summary, the proposed chaotic PRNG is a promising candidate for practical applications. Further comparison with different state-of-the-art PRNG schemes in terms of computational complexity, storage requirement, communication cost, etc., it will be carried out in future research along the same lines.

References

[1] Li, Tien Yien, James A Yorke. Period three implies chaos. *The American Mathematical Monthly* 82.10 (1975): 985-992.
[2] Rong, Chen Guan, Dong Xiao Ning. From chaos to order: methodologies, perspectives and applications. World Scientific, 1998.
[3] Sprott, Julien Clinton, Julien C. Sprott. Chaos and time-series analysis. Vol. 69. Oxford: Oxford University Press, 2003.
[4] Pecora, Louis M, Thomas L. Carroll. Synchronization in chaotic systems. *Physical review letters.* 1990; 64(8): 821-825.
[5] Murali, K, M Lakshmanan. Secure communication using a compound signal from generalized synchronizable chaotic systems. *Physics Letters A*. 1998; 241(6): 303-310.
[6] Abdurahman, Kadir, Wang Xing-Yuan, Zhao Yu-Zhang. Generalized synchronization of diverse structure chaotic systems. *Chinese Physics Letters.* 2011; 28(9): 090503.
[7] Margheri, Alessandro, Rogério Martins. Generalized synchronization in linearly coupled time periodic systems. *Journal of Differential Equations* 249. 2010; 12: 3215-3232.
[8] Zhi-Ling, Yuan, Xu Zhen-Yuan, Guo Liu-Xiao. Generalized synchronization of two unidirectionally coupled discrete stochastic dynamical systems. *Chinese physics B* 20.7 2011: 070503.
[9] Koronovskii, AA, OI Moskalenko, AE Hramov. Generalized synchronization in complex networks. *Technical Physics Letters*, 2012; 38(10): 924-927.
[10] Min, Lequan, Guanrong Chen. Generalized synchronization in an array of nonlinear dynamic systems with applications to chaotic CNN. *International Journal of Bifurcation and Chaos*, 2013: 1350016.
[11] Jia, Qianqian. Synchronization Control of Complex Dynamical Networks Based on Uncertain Coupling. *TELKOMNIKA (Telecommunication Computing Electronics and Control).* 2017; 15(3): 1164-1172.
[12] Zang, Hongyan, Lequan Min, Geng Zhao. *A generalized synchronization theorem for discrete-time chaos system with application in data encryption scheme*. Communications, Circuits and Systems, 2007. ICCCAS 2007. International Conference on. IEEE, 2007.
[13] Wang, Yong, et al. A new chaos-based fast image encryption algorithm. *Applied soft computing.* 2011; 11(1): 514-522.
[14] Kanso, A, M Ghebleh. A novel image encryption algorithm based on a 3D chaotic map. *Communications in Nonlinear Science and Numerical Simulation.* 2012; 17(7): 2943-2959.
[15] Min, Lequan, et al. *Study on pseudorandomness of some pseudorandom number generators with application*. Computational Intelligence and Security (CIS), 2013 9th International Conference on. IEEE, 2013.
[16] Guo, Cheng, Chin-Chen Chang, Chin-Yu Sun. Chaotic maps-based mutual authentication and key agreement using smart cards for wireless communications. *Journal of Information Hiding and Multimedia Signal Processing*. 2013; 4(2): 99-109.
[17] Liu, Yang, Xiaojun Tong, Shicheng Hu. A family of new complex number chaotic maps based image encryption algorithm. *Signal Processing: Image Communication*, 2013; 28(10): 1548-1559.
[18] Du, Baoxiang, Qun Ding, Xiaoli Geng Analysis and elimination of digital chaotic key sequence's autocorrelation. *Journal of Information Hiding and Multimedia Signal Processing*, (2014); 5(2): 302-309.
[19] Min, Lequan, et al. Some polynomial chaotic maps without equilibria and an application to image encryption with avalanche effects. *International Journal of Bifurcation and Chaos,* 2015; 25(09): 1550124.
[20] Han, Dandan, Lequan Min, Guanrong Chen. A Stream Encryption Scheme with Both Key and Plaintext Avalanche Effects for Designing Chaos-Based Pseudorandom Number Generator with

Application to Image Encryption. *International Journal of Bifurcation and Chaos*, (2016); 26 (05): 1650091.
[21] Sukirman, Edi, MT Suryadi, M Agus Mubarak. The implementation of henon map algorithm for digital image encryption. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2014; 12(3): 651-656.
[22] Arboleda, Edwin R, Joel L Balaba, John Carlo L Espineli. Chaotic Rivest-Shamir-Adlerman Algorithm with Data Encryption Standard Scheduling. *Bulletin of Electrical Engineering and Informatics* (*BEEI).* 2017; 6(3): 219-227.
[23] Pacha, Adda Ali, Naima Hadj Said. The quality of a New Generator sequence improvent for spreading the Color Image Transmission system. *TELKOMNIKA (Telecommunication Computing Electronics and Control),* 2018; 16(1): 402~414.
[24] Xiao, Genfu, et al. Research on Chaotic Firefly Algorithm and the Application in Optimal Reactive Power Dispatch. *TELKOMNIKA (Telecommunication Computing Electronics and Control),* 2017; 15(1); 93-100.
[25] Wang, Junnian, et al. The Chaos and Stability of Firefly Algorithm Adjacent Individual. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2017; 15(4): 1733~1740.
[26] Spillman, Richard J. *Classical and contemporary cryptology*. Prentice-Hall, Inc., 2004.
[27] Feistel, Horst. Cryptography and computer privacy. *Scientific American*. 1973; 228(5): 15-23.
[28] Min, Lequan, and Guanrong Chen. A novel stream encryption scheme with avalanche effect. *The European Physical Journal B*. 2013; 86(459): 1-13.
[29] Chen, E, Lequan Min, Guanrong Chen. Discrete Chaotic Systems with One-Line Equilibria and Their Application to Image Encryption. *International Journal of Bifurcation and Chaos*, 2017: 27(03): 1750046.
[30] Zhang, Mei, et al. A generalized stability theorem for discrete-time nonautonomous chaos system with applications. *Mathematical Problems in Engineering.* 2015.
[31] Fiedler, Bernold, Stefan Liebscher. Bifurcations without parameters: Some ODE and PDE examples. arXiv preprint math/0304453(2003).
[32] FIPS, PUB. 140-2. Security Requirements for Cryptographic Modules, 2001; 25.
[33] ETSI/SAGE Specification, Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 2: ZUC Specification; Version: 1.5, Date: 4th January 2011.
[34] Breve, Fabricio A., et al. Chaotic phase synchronization and desynchronization in an oscillator network for object selection. *Neural Networks*, 2009; 22(5): 728-737
[35] Kocarev, Lj, U Parlitz. Generalized synchronization, predictability, and equivalence of unidirectionally coupled dynamical systems. *Physical review letters*, 1996; 76(11): 1816.
[36] Min, Lequan, Tianyu Chen, Hongyan Zang. Analysis of fips 140-2 test and chaos-based pseudorandom number generator. *Chaotic Modeling and Simulation*x, 2013; 76(11): 273-280.
[37] Min, Lequan, Tianyu Chen, Hongyan Zang. Analysis of fips 140-2 test and chaos-based pseudorandom number generator. *Chaotic Modeling and Simulation*, 2013; 2(1): 273-280.
[38] Golomb, Solomon W. SHIFT REGISTER SEQUENCES: Secure and Limited-Access Code Generators, Efficiency Code Generators, Prescribed Property Generators, Mathematical Models. 1982.